

ELECTRONIC SECURITY COMPONENT

Field of the Invention

The present invention relates to electronic devices, and, more particularly, to an electronic security component in which sensitive information is
5 processed.

Background of the Invention

Electronic security components processing sensitive information are used especially in smart cards. Applications of these cards include accessing
10 banks for banking applications, and for remote payments for television, gasoline distribution and highway tolls, for example. These electronic security components have to process confidential data that must be shielded against any attempt at espionage for
15 fraudulent purposes. The confidential data travels through the data bus of the component between a central processing unit (processor) and peripherals, such as memories.

Different methods can be implemented to
20 discover these confidential data elements. In particular, one physical characteristic that can be observed external the electronic component is its current signature which depends on the passage of data in transit on the data bus. The data bus has a high

capacity because it circulates throughout the component.

For this reason, the output interface includes three-state selection switches sized to let
5 through high current for charging or discharging the line capacitor. Since the data bus is an 8-bit data bus, it includes eight large selector switches that are activated to apply a data element to this bus. Consequently, there is high current consumption during
10 the selection switching of the switches.

Summary of the Invention

In view of the foregoing background, it is an object of the present invention to prevent the identification of data elements traveling through the
15 bus or at least make this identification difficult.

It is another object of the present invention to use data encryption to improve the protection of confidential data.

Yet another object of the present invention
20 is to implement data encryption at low cost whether in terms of silicon surface area, connection lines between the peripherals and the central processing unit, or data-processing time.

Another object of the present invention is to
25 implement a data encryption system that can be adapted to all classes of components in a relatively straight forward manner without extra cost of customized design.

In view of these and other objects, advantages and features, one approach is to provide a
30 component whose central processing unit and peripherals, which have to process sensitive data received or transmitted on the data bus, each comprise an encryption/decryption cell. Each encryption/decryption cell applies the same secret key
35 produced locally by each cell at each clock cycle to a

data element received or to be transmitted in the clock cycle.

Using the convention according to a clock cycle starting at the high level, the writing of a data element of the bus is done at the low level and the reading of a data element on the bus is done on the leading edge. Thus, in a given clock cycle, a data element may be encrypted with a secret key produced by the cell of a sender and transmitted on the bus during the write period on the bus. This encrypted data element may be read by an addressee and decrypted in the cell of this addressee with the secret key locally produced by this cell.

The two locally produced secret keys have the particular feature of being identical. Thus, according to the invention, the secret key is produced locally in each cell from a synchronous random signal applied to all. This is done in one clock cycle for the encryption of a data element given by a sender, and for the decryption of this data element encrypted by an addressee.

The present invention therefore relates to an electronic component comprising a two-way bus through which data elements travel in transit between peripherals and a central processing unit at the rate of a clock signal. The central processing unit and at least one of the peripherals each comprises a data encryption/decryption cell using the same secret key. A current value of the secret key is produced locally in each cell at each clock cycle from a random signal synchronous with the clock signal, and is applied to each of the cells by a one-way transmission line.

Brief Description of the Drawings

Other features and advantages of the invention shall be described in detail in the following

description by way of a non-restricted indication and with reference to the appended figures, of which:

Figure 1 shows an exemplary architecture of an electronic component to which the present invention
5 can be applied;

Figure 2 shows a simplified architecture of an electronic component according to the present invention;

Figure 3 is an exemplary timing diagram of
10 the data and control signals of the electronic component shown in Figure 2;

Figure 4 is a block diagram of an encryption/decryption cell according to the present invention;

Figure 5 shows the encryption/decryption cell comprising a conditional circuit applicable to the central processing unit according to the present
15 invention;

Figure 6 is a detailed drawing of the encryption and decryption circuits in the cell
20 according to the present invention; and

Figure 7 is a block diagram of a synchronous random signal generator that can be used in the present invention.

25 Detailed Description of the Preferred Embodiments

Figure 1 shows an exemplary architecture of an electronic security component to which the present invention can be applied. In this example, the electronic component is more particularly designed for
30 smart card type applications. Its external connections are thus limited to two series-connected input/output pads, a clock pad CALK to receive an external clock signal, a pad to receive a resetting signal RST, and the logic supply pads Vcc and Gnd.

35 The architecture of this component comprises a central processing unit CPU and peripherals P1, P2,

P3 which, in the example, are respectively a non-volatile memory (e.g., an EEPROM type), a RAM type working memory, and a ROM type program memory. An interface circuit INT provides the interface between
5 the serial input/output pads and the parallel bus of the component which is subdivided into an address bus AD-BUS, and a data bus DATA-BUS to which the central processing unit and the peripherals are connected.

In this architecture, it is also planned to
10 have a circuit CAP for access control to the peripheral which receives the most significant bits A7-A5 from the address bus AD-BUS. It contains a space allocation table for the physical addressable space of the component and gives especially the selection signals
15 P1-sel, P2-sel and P3-sel of the peripherals P1, P2, P3 as a function of the decoded address. In this example, the peripherals receive only the least significant bits A5-A0 from the address bus.

Depending on the instructions that the
20 central processing unit receives externally, it gives control signals CTL, especially a read/write signal RW, to be applied to the peripherals. Finally, the pad CALK gives the clock signal PHI applied to all the circuits of the component. That is, the clock signal
25 PHI is applied to the central processing unit, the peripherals, the interface circuit, and the peripheral access control circuit in the example.

In the invention, it is sought to secure this circuit by preventing the determining of the data
30 elements that travel through the internal data bus DATA-BUS through observation of the current consumption of the component. Thus, as shown in Figure 2 in a simplified representation of the architecture of the component of Figure 1, an encryption/decryption cell is
35 placed in the central processing unit and in each of the peripherals that read or write sensitive data on the data bus, i.e., in the peripherals P1 and P2.

These cells are referenced Kcell_{cpu}, Kcell_{p1} and Kcell_{p2} in Figure 2.

The electronic component according to the invention then comprises a random signal generator
5 KEY_GEN synchronized with a clock signal on a one-way transmission line to apply this signal to each of the encryption/decryption cells planned in the component. Each of these cells is furthermore connected to the input/output of the data bus DATA-BUS.

10 Figure 3 shows a timing diagram corresponding to a read operation in which the central processing unit reads a data element of the peripheral P1 followed by a write operation in which the central processing unit writes the data element in the peripheral P1. This
15 timing diagram illustrates the principle of the invention.

This timing diagram shows two clock cycles referenced cycle 1 and cycle 2, the synchronous random signal K_{IN}, the secret key KEY computed locally in each
20 cell, the address bus AD-BUS, the selection signal P1-sel of the peripheral P1, the read/write control signal RW whose low level corresponds to a write command and whose high level corresponds to a read command (by convention), and the data bus DATA-BUS. Considering
25 the first clock cycle shown (cycle 1), it has a corresponding value KEY₀ of the secret key that is computed locally in each cell from the new input value of the random signal K_{IN}, which is 0 in the example.

The peripheral P1 is selected (P1-sel at the
30 high level) in read mode (RW at the high level) at the address applied to the address bus AD-BUS. The cell Kcell_{p1} of peripheral P1 gives on the bus the data element read at this address, which is encrypted with the current value of the secret key KEY₀ that is
35 locally computed by this cell Kcell_{p1}. This data element is transmitted on the bus on the low level of the cycle 1 of the clock signal. The encrypted data

element is stored in an input register of the central processing unit CPU on the leading edge of the cycle 1 of the clock signal, and decrypted by the cell Kcell_{CPU} with the current value KEY₀ of the secret key locally computed by this cell Kcell_{CPU}.

Considering the second clock cycle shown (cycle 2), it has a corresponding value KEY₁ of the secret key locally computed in each cell from the new input value of the random key KIN, which is 1 in the example. The peripheral P1 is selected (P1-sel at the high level) in write mode (RW at the low level) at the address applied to the address bus AD-BUS. The cell Kcell_{CPU} of the central processing unit gives on the bus the data element to be written at this address, which is encrypted with the current value of secret key KEY₁ that is locally computed by this cell Kcell_{CPU}. This data element is transmitted on the bus on the low level of the cycle 2 of the clock signal. The encrypted data element is stored in an input register of the peripheral P1 on the leading edge of the cycle 2 of the clock signal, and decrypted by the cell Kcell_{P1} with the current value KEY₁ of the secret key locally computed by this cell Kcell_{P1}.

A general block diagram of an encryption/ decryption cell Kcell according to the invention is shown in Figure 4. This cell is such that it locally computes the current value of the secret key used both for encryption and for decryption. The cell Kcell has a register KEYREG that gives the secret key KEY for the encryption and decryption. It is an n-stage shift register sequenced by the clock signal PHI and receives the random data signal KIN at input synchronous with the clock signal PHI. The register KEYREG gives the current value of the secret key KEY at output for the current clock cycle, whose value is a polynomial function of the n most recent values of the random signal KIN. The

secret key thus takes a new random value at each clock cycle.

The register is preferably a feedback shift register. That is to say, it has combinational logic gates to apply the output bit of certain stages to the input of other stages of the register. This makes it possible to obtain valuable polynomial functions. Preferably, an irreducible polynomial function is implemented to improve the resistance of the encryption.

The cell Kcell has an encryption module A and a decryption module B to which the secret key KEY given by the register KEYREG of the cell is applied. In the example, the mathematical function implemented in the encryption module is the XOR function which has the particular feature of being also the function to be applied in the decryption module and of being easy to implement.

The encryption module A receives inter alia an internal data element Dout from the circuit in which the cell Kcell is placed and the secret key KEY produced locally by the register KEYREG. At output, it delivers an encrypted data element applied to the data bus DATA-BUS through the output interface of the circuit, which is symbolically shown in the figure by a controlled inverter.

The decryption module B receives a data element from the data bus and the secret key KEY locally produced by the register KEYREG. At output, it gives a decrypted data element Din. In one improvement shown in Figure 5, the encryption/decryption cell of the central processing unit comprises, in addition to the elements described here above, a conditional circuit used for the application to the encryption and decryption modules of either the secret key KEY or a neutral key KN corresponding to the neutral value for

the encryption operation considered. In the exemplary XOR operation, this neutral value is the zero value.

This improvement is used to avoid implementing an encryption/decryption cell in all the circuits connected to the data bus in the component considered, and is implemented in only those cells that handle data elements to be protected. It is therefore planned that the control circuit PAC for access to the peripherals (shown in Figures 1 and 2) will give an encryption enabling signal SCRAMBLE to the central processing unit CPU whenever it decodes the address of a peripheral of this kind. In practice, this access control circuit finds this information in its physical address allocation table.

It will be noted that the information SCRAMBLE in the example given by the access control circuit is placed outside or external the central processing unit in the exemplary architecture shown in Figures 1 and 2. This is not absolutely restrictive. The information SCRAMBLE is more generally given by an address decoding circuit of the component.

The conditional circuit of the cell Kcell_{cpu} according to the improvement of the invention comprises a multiplexer MUX receiving the secret key KEY and the neutral key KN at input. At output, this conditional circuit gives the key selected by the encryption enabling signal SCRAMBLE, which is applied to the encryption and decryption modules of this cell Kcell_{cpu}.

Figure 6 gives a slightly more detailed view of an encryption/decryption cell according to the present invention. If we consider an 8-bit data bus, the secret key must include at least as many bits. The register KEYREG has eight stages to give eight secret key bits referenced K0 to K7. Each of these eight data bits is applied in the encryption module A, and in the decryption module B to a corresponding XOR gate

receiving the same-order data bit to be encrypted or decrypted at input. Each of these modules thus comprises eight XOR gates, one per bit.

This figure shows an exemplary embodiment of a shift type feedback register KEYREG. The references E0 to E7 designate the eight stages of the register, respectively giving the bits K7 to K0 of the secret key. These stages may be D-type flip-flop circuits, for example.

In the exemplary embodiment shown, the stage E0 receives at input the random signal KIN combined in an XOR gate with the bit K0 given by the last stage E7 of the register, and at output it delivers the bit K7. The stage E1 receives at input the bit K7 combined in an XOR gate with the bit K0. At output it delivers the bit K6. The stages E2, E3 and E4 receive at input the bits given by the preceding stage, and deliver at output the bits K5, K4 and K3 respectively. The stage E5 receives the bit K3 at input which is combined in an XOR gate with the bit K0, and delivers the bit K2 at output. This stage E6 receives the bit K2 at input which is combined in an XOR gate with the bit K0, and delivers the bit K1 at output. The stage E7 receives the bit K1 at input and delivers the bit K0 at output.

Figure 7 represents an exemplary generator KEYGEN of the random signal KIN. In this example, the generator comprises a pseudo-random generator to give a random clock signal that is applied to the D input of a flip-flop circuit BS to be synchronized by the clock signal PHI. This flip-flop circuit therefore receives the clock signal PHI at its clock input, and gives at its Q output a random signal KIN that is synchronized with the clock signal PHI.

It is very difficult in principle to determine the value taken by the random signal by observing the power consumption of the component arising from the switching operations on the

transmission line of the synchronous random signal KIN because the capacitance of this one-way line is very low. However, in one improvement of the invention, it is planned that the generator of the synchronous random
5 signal will comprise a circuit CMC for masking the consumption due to the selection switching operations on this transmission line. In the example, this circuit CMC is connected between the output of the synchronization flip-flop circuit BS and the
10 transmission line.

There are different consumption masking circuits of varying degrees of efficiency. An exemplary non-exhaustive embodiment is shown in Figure 7. It has two D-type flip-flop circuits, B1 and
15 B2. The first flip-flop circuit B1 receives the Q output of the synchronization flip-flop circuit BS as a data input, and the clock signal from the bus PHI as a clock input. The Q output is connected by an interface element (driver) I1 to the transmission line.

20 The complementary /Q output of the flip-flop circuit B1 is applied to a combinational circuit whose output S is applied to the data input of the second flip-flop circuit B2. The Q output of this second flip-flop circuit B2 is connected to a capacitor CKN
25 whose capacitance corresponds to the parasitic capacitance CK of the transmission line perceived by the output interface I1 of the generator KEYGEN.

The combinational circuit, in the example, has a first OR gate receiving the Q outputs of the
30 synchronization flip-flop circuit and of the second flip-flop circuit B2 as inputs. A second OR gate receives the output of the first gate and the complementary output /Q of the first flip-flop circuit B1 as inputs. With a combinational circuit of this
35 kind, complementary transitions are obtained in the flip-flop circuits B1 and B2 so that the same

consumption due to the transmission of the signal KIN is observed at each clock cycle.

In a another improvement of the invention, it is planned that the random signal KIN will be
5 transmitted on the transmission line only after activation by the central processing unit of an encryption activation signal EN-ENCRYPT. This can be done simply by forcing the resetting of the flip-flop circuits.

10 Figure 7 thus shows an AND type logic gate receiving, as inputs, the resetting signal RST of the component which is active at zero, and the enabling signal EN-ENCRYPT. This signal is at zero by default. Thus, so long as the enabling signal is at zero after
15 the setting, the flip-flop circuits B1 and B2 are set at zero, and the transmission line is set at zero. As soon as it is set at 1 by the central processing unit, the random signal is sent.

It will be noted that the two improvements of
20 the generator of the synchronous random signal, namely the masking of consumption and the enabling of encryption, can be implemented independently of each other. Thus, in certain components, it is possible to implement only one of these improvements. To this end,
25 it will be noted that the improvement relating to encryption enabling can be implemented independently of the masking circuit. For example, this may be done using an AND logic gate receiving the synchronous random signal KIN and the activation signal EN-ENCRYPT as
30 inputs, and connected at output to the transmission line.

The use of encryption/decryption cells according to the invention thus gives efficient protection for sensitive data. This protection costs
35 little in terms of design, implementation and processing time for the component. In particular, the design is facilitated by the user of encryption/

decryption cells that are identical in all the peripherals.

The encryption/decryption cell of the central processing unit comprises an encryption-enabling option
5 by which it is possible not to implant a cell necessarily in all the peripherals. The random signal generator has two embodiment options, which are a consumption masking option and an encryption/decryption activation option.

27 1
28 2
29 3
30 4
31 5
32 6
33 7
34 8
35 9
36 10
37 11
38 12
39 13
40 14
41 15
42 16
43 17
44 18
45 19
46 20
47 21
48 22
49 23
50 24
51 25
52 26
53 27
54 28
55 29
56 30
57 31
58 32
59 33
60 34
61 35
62 36
63 37
64 38
65 39
66 40
67 41
68 42
69 43
70 44
71 45
72 46
73 47
74 48
75 49
76 50
77 51
78 52
79 53
80 54
81 55
82 56
83 57
84 58
85 59
86 60
87 61
88 62
89 63
90 64
91 65
92 66
93 67
94 68
95 69
96 70
97 71
98 72
99 73
100 74
101 75
102 76
103 77
104 78
105 79
106 80
107 81
108 82
109 83
110 84
111 85
112 86
113 87
114 88
115 89
116 90
117 91
118 92
119 93
120 94
121 95
122 96
123 97
124 98
125 99
126 100
127 101
128 102
129 103
130 104
131 105
132 106
133 107
134 108
135 109
136 110
137 111
138 112
139 113
140 114
141 115
142 116
143 117
144 118
145 119
146 120
147 121
148 122
149 123
150 124
151 125
152 126
153 127
154 128
155 129
156 130
157 131
158 132
159 133
160 134
161 135
162 136
163 137
164 138
165 139
166 140
167 141
168 142
169 143
170 144
171 145
172 146
173 147
174 148
175 149
176 150
177 151
178 152
179 153
180 154
181 155
182 156
183 157
184 158
185 159
186 160
187 161
188 162
189 163
190 164
191 165
192 166
193 167
194 168
195 169
196 170
197 171
198 172
199 173
200 174
201 175
202 176
203 177
204 178
205 179
206 180
207 181
208 182
209 183
210 184
211 185
212 186
213 187
214 188
215 189
216 190
217 191
218 192
219 193
220 194
221 195
222 196
223 197
224 198
225 199
226 200
227 201
228 202
229 203
230 204
231 205
232 206
233 207
234 208
235 209
236 210
237 211
238 212
239 213
240 214
241 215
242 216
243 217
244 218
245 219
246 220
247 221
248 222
249 223
250 224
251 225
252 226
253 227
254 228
255 229
256 230
257 231
258 232
259 233
260 234
261 235
262 236
263 237
264 238
265 239
266 240
267 241
268 242
269 243
270 244
271 245
272 246
273 247
274 248
275 249
276 250
277 251
278 252
279 253
280 254
281 255
282 256
283 257
284 258
285 259
286 260
287 261
288 262
289 263
290 264
291 265
292 266
293 267
294 268
295 269
296 270
297 271
298 272
299 273
300 274
301 275
302 276
303 277
304 278
305 279
306 280
307 281
308 282
309 283
310 284
311 285
312 286
313 287
314 288
315 289
316 290
317 291
318 292
319 293
320 294
321 295
322 296
323 297
324 298
325 299
326 300
327 301
328 302
329 303
330 304
331 305
332 306
333 307
334 308
335 309
336 310
337 311
338 312
339 313
340 314
341 315
342 316
343 317
344 318
345 319
346 320
347 321
348 322
349 323
350 324
351 325
352 326
353 327
354 328
355 329
356 330
357 331
358 332
359 333
360 334
361 335
362 336
363 337
364 338
365 339
366 340
367 341
368 342
369 343
370 344
371 345
372 346
373 347
374 348
375 349
376 350
377 351
378 352
379 353
380 354
381 355
382 356
383 357
384 358
385 359
386 360
387 361
388 362
389 363
390 364
391 365
392 366
393 367
394 368
395 369
396 370
397 371
398 372
399 373
400 374
401 375
402 376
403 377
404 378
405 379
406 380
407 381
408 382
409 383
410 384
411 385
412 386
413 387
414 388
415 389
416 390
417 391
418 392
419 393
420 394
421 395
422 396
423 397
424 398
425 399
426 400
427 401
428 402
429 403
430 404
431 405
432 406
433 407
434 408
435 409
436 410
437 411
438 412
439 413
440 414
441 415
442 416
443 417
444 418
445 419
446 420
447 421
448 422
449 423
450 424
451 425
452 426
453 427
454 428
455 429
456 430
457 431
458 432
459 433
460 434
461 435
462 436
463 437
464 438
465 439
466 440
467 441
468 442
469 443
470 444
471 445
472 446
473 447
474 448
475 449
476 450
477 451
478 452
479 453
480 454
481 455
482 456
483 457
484 458
485 459
486 460
487 461
488 462
489 463
490 464
491 465
492 466
493 467
494 468
495 469
496 470
497 471
498 472
499 473
500 474
501 475
502 476
503 477
504 478
505 479
506 480
507 481
508 482
509 483
510 484
511 485
512 486
513 487
514 488
515 489
516 490
517 491
518 492
519 493
520 494
521 495
522 496
523 497
524 498
525 499
526 500
527 501
528 502
529 503
530 504
531 505
532 506
533 507
534 508
535 509
536 510
537 511
538 512
539 513
540 514
541 515
542 516
543 517
544 518
545 519
546 520
547 521
548 522
549 523
550 524
551 525
552 526
553 527
554 528
555 529
556 530
557 531
558 532
559 533
560 534
561 535
562 536
563 537
564 538
565 539
566 540
567 541
568 542
569 543
570 544
571 545
572 546
573 547
574 548
575 549
576 550
577 551
578 552
579 553
580 554
581 555
582 556
583 557
584 558
585 559
586 560
587 561
588 562
589 563
590 564
591 565
592 566
593 567
594 568
595 569
596 570
597 571
598 572
599 573
600 574
601 575
602 576
603 577
604 578
605 579
606 580
607 581
608 582
609 583
610 584
611 585
612 586
613 587
614 588
615 589
616 590
617 591
618 592
619 593
620 594
621 595
622 596
623 597
624 598
625 599
626 600
627 601
628 602
629 603
630 604
631 605
632 606
633 607
634 608
635 609
636 610
637 611
638 612
639 613
640 614
641 615
642 616
643 617
644 618
645 619
646 620
647 621
648 622
649 623
650 624
651 625
652 626
653 627
654 628
655 629
656 630
657 631
658 632
659 633
660 634
661 635
662 636
663 637
664 638
665 639
666 640
667 641
668 642
669 643
670 644
671 645
672 646
673 647
674 648
675 649
676 650
677 651
678 652
679 653
680 654
681 655
682 656
683 657
684 658
685 659
686 660
687 661
688 662
689 663
690 664
691 665
692 666
693 667
694 668
695 669
696 670
697 671
698 672
699 673
700 674
701 675
702 676
703 677
704 678
705 679
706 680
707 681
708 682
709 683
710 684
711 685
712 686
713 687
714 688
715 689
716 690
717 691
718 692
719 693
720 694
721 695
722 696
723 697
724 698
725 699
726 700
727 701
728 702
729 703
730 704
731 705
732 706
733 707
734 708
735 709
736 710
737 711
738 712
739 713
740 714
741 715
742 716
743 717
744 718
745 719
746 720
747 721
748 722
749 723
750 724
751 725
752 726
753 727
754 728
755 729
756 730
757 731
758 732
759 733
760 734
761 735
762 736
763 737
764 738
765 739
766 740
767 741
768 742
769 743
770 744
771 745
772 746
773 747
774 748
775 749
776 750
777 751
778 752
779 753
780 754
781 755
782 756
783 757
784 758
785 759
786 760
787 761
788 762
789 763
790 764
791 765
792 766
793 767
794 768
795 769
796 770
797 771
798 772
799 773
800 774
801 775
802 776
803 777
804 778
805 779
806 780
807 781
808 782
809 783
810 784
811 785
812 786
813 787
814 788
815 789
816 790
817 791
818 792
819 793
820 794
821 795
822 796
823 797
824 798
825 799
826 800
827 801
828 802
829 803
830 804
831 805
832 806
833 807
834 808
835 809
836 810
837 811
838 812
839 813
840 814
841 815
842 816
843 817
844 818
845 819
846 820
847 821
848 822
849 823
850 824
851 825
852 826
853 827
854 828
855 829
856 830
857 831
858 832
859 833
860 834
861 835
862 836
863 837
864 838
865 839
866 840
867 841
868 842
869 843
870 844
871 845
872 846
873 847
874 848
875 849
876 850
877 851
878 852
879 853
880 854
881 855
882 856
883 857
884 858
885 859
886 860
887 861
888 862
889 863
890 864
891 865
892 866
893 867
894 868
895 869
896 870
897 871
898 872
899 873
900 874
901 875
902 876
903 877
904 878
905 879
906 880
907 881
908 882
909 883
910 884
911 885
912 886
913 887
914 888
915 889
916 890
917 891
918 892
919 893
920 894
921 895
922 896
923 897
924 898
925 899
926 900
927 901
928 902
929 903
930 904
931 905
932 906
933 907
934 908
935 909
936 910
937 911
938 912
939 913
940 914
941 915
942 916
943 917
944 918
945 919
946 920
947 921
948 922
949 923
950 924
951 925
952 926
953 927
954 928
955 929
956 930
957 931
958 932
959 933
960 934
961 935
962 936
963 937
964 938
965 939
966 940
967 941
968 942
969 943
970 944
971 945
972 946
973 947
974 948
975 949
976 950
977 951
978 952
979 953
980 954
981 955
982 956
983 957
984 958
985 959
986 960
987 961
988 962
989 963
990 964
991 965
992 966
993 967
994 968
995 969
996 970
997 971
998 972
999 973
1000 974
1001 975
1002 976
1003 977
1004 978
1005 979
1006 980
1007 981
1008 982
1009 983
1010 984
1011 985
1012 986
1013 987
1014 988
1015 989
1016 990
1017 991
1018 992
1019 993
1020 994
1021 995
1022 996
1023 997
1024 998
1025 999
1026 1000
1027 1001
1028 1002
1029 1003
1030 1004
1031 1005
1032 1006
1033 1007
1034 1008
1035 1009
1036 1010
1037 1011
1038 1012
1039 1013
1040 1014
1041 1015
1042 1016
1043 1017
1044 1018
1045 1019
1046 1020
1047 1021
1048 1022
1049 1023
1050 1024
1051 1025
1052 1026
1053 1027
1054 1028
1055 1029
1056 1030
1057 1031
1058 1032
1059 1033
1060 1034
1061 1035
1062 1036
1063 1037
1064 1038
1065 1039
1066 1040
1067 1041
1068 1042
1069 1043
1070 1044
1071 1045
1072 1046
1073 1047
1074 1048
1075 1049
1076 1050
1077 1051
1078 1052
1079 1053
1080 1054
1081 1055
1082 1056
1083 1057
1084 1058
1085 1059
1086 1060
1087 1061
1088 1062
1089 1063
1090 1064
1091 1065
1092 1066
1093 1067
1094 1068
1095 1069
1096 1070
1097 1071
1098 1072
1099 1073
1100 1074
1101 1075
1102 1076
1103 1077
1104 1078
1105 1079
1106 1080
1107 1081
1108 1082
1109 1083
1110 1084
1111 1085
1112 1086
1113 1087
1114 1088
1115 1089
1116 1090
1117 1091
1118 1092
1119 1093
1120 1094
1121 1095
1122 1096
1123 1097
1124 1098
1125 1099
1126 1100
1127 1101
1128 1102
1129 1103
1130 1104
1131 1105
1132 1106
1133 1107
1134 1108
1135 1109
1136 1110
1137 1111
1138 1112
1139 1113
1140 1114
1141 1115
1142 1116
1143 1117
1144 1118
1145 1119
1146 1120
1147 1121
1148 1122
1149 1123
1150 1124
1151 1125
1152 1126
1153 1127
1154 1128
1155 1129
1156 1130
1157 1131
1158 1132
1159 1133
1160 1134
1161 1135
1162 1136
1163 1137
1164 1138
1165 1139
1166 1140
1167 1141
1168 1142
1169 1143
1170 1144
1171 1145
1172 1146
1173 1147
1174 1148
1175 1149
1176 1150
1177 1151
1178 1152
1179 1153
1180 1154
1181 1155
1182 1156
1183 1157
1184 1158
1185 1159
1186 1160
1187 1161
1188 1162
1189 1163
1190 1164
1191 1165
1192 1166
1193 1167
1194 1168
1195 1169
1196 1170
1197 1171
1198 1172
1199 1173
1200 1174
1201 1175
1202 1176
1203 1177
1204 1178
1205 1179
1206 1180
1207 1181
1208 1182
1209 1183
1210 1184
1211 1185
1212 1186
1213 1187
1214 1188
1215 1189
1216 1190
1217 1191
1218 1192
1219 1193
1220 1194
1221 1195
1222 1196
1223 1197
1224 1198
1225 1199
1226 1200
1227 1201
1228 1202
1229 1203
1230 1204
1231 1205
1232 1206
1233 1207
1234 1208
1235 1209
1236 1210
1237 1211
1238 1212
1239 1213
1240 1214
1241 1215
1242 1216
1243 1217
1244 1218
1245 1219
1246 1220
1247 1221
1248 1222
1249 1223
1250 1224
1251 1225
1252 1226
1253 1227
1254 1228
1255 1229
1256 1230
1257 1231
1258 1232
1259 1233
1260 1234
1261 1235
1262 1236
1263 1237
1264 1238
1265 1239
1266 1240
1267 1241
1268 1242
1269 1243
1270 1244
1271 1245
1272 1246
1273 1247
1274 1248
1275 1249
1276 1250
1277 1251
1278 1252
1279 1253
1280 1254
1281 1255
1282 1256
1283 1257
1284 1258
1285 1259
1286 1260
1287 1261
1288 1262
1289 1263
1290 1264
1291 1265
1292 1266
1293 1267
1294 1268
1295 1269
1296 1270
1297 1271
1298 1272
1299 1273
1300 1274
1301 1275
1302 1276
1303 1277
1304 1278
1305 1279
1306 1280
1307 1281
1308 1282
1309 1283
1310 1284
1311 1285
1312 1286
1313 1287
1314 1288
1315 1289
1316 1290
1317 1291
1318 1292
1319 1293
1320 1294
1321 1295
1322 1296
1323 1297
1324 1298
1325 1299
1326 1300
1327 1301
1328 1302
1329 1303
1330 1304